

AIR WAR COLLEGE

AIR UNIVERSITY

TOWARD CYBER OMNISCIENCE:  
DETECTING CYBER ATTACKS  
BY HOSTILE INDIVIDUALS IN 2035

by

William P. Jensen, Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

Distribution A: Approved for public release; distribution unlimited.

## **DISCLAIMER**

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

## Contents

Disclaimer .....	i
Contents .....	ii
Biography .....	iii
A Corrupted iCon: A Life Lost in 2035 .....	iv
Introduction .....	1
Convergence of People and Technology in 2035 .....	6
The Cyber Threat: The Hostile Individual .....	12
Toward Cyber Omniscience: Deterring the Individual in 2035 .....	14
Is This 2035 ... Or <i>1984</i> ? .....	18
Policy Recommendations: Getting Ahead of the Future .....	21
Conclusion .....	24
Bibliography .....	27

## **Biography**

Colonel William P. Jensen graduated in 1990 from The Florida State University, receiving a Bachelor of Science degree in Computer and Information Sciences. He received a Master of Arts in Religion, “Summa Cum Laude,” from Liberty University in 2000 and a Master of Military Art and Science from the U.S. Army School of Advanced Military Studies in 2005.

Colonel Jensen attended Specialized Undergraduate Navigator Training at Mather AFB, California, in 1990. His first assignment was with the 38<sup>th</sup> Reconnaissance Squadron (RS), Offutt AFB, Omaha, Nebraska, from 1992-1997. His next assignment was with the 55<sup>th</sup> Operations Group, Offutt AFB, 1997-1998, where he served as the group RC-135 Evaluator Navigator, and was the focal point for all RC-135 issues. Colonel Jensen transitioned to the 562d Flying Training Squadron, Joint Specialized Undergraduate Navigator Training, Randolph AFB, San Antonio, Texas, in 1998. In 2001, Colonel Jensen was selected to command Cadet Squadron Eleven at the United States Air Force Academy, Colorado Springs, Colorado. Following command, Colonel Jensen served as the Commandant’s Executive Officer until 2003. Colonel Jensen was selected to attend the U.S. Army Command and General Staff College and School of Advanced Military Studies, Ft. Leavenworth, Kansas. In 2005, Colonel Jensen was assigned to the 608<sup>th</sup> Combat Plans Squadron as the Chief of Strategy for 8<sup>th</sup> Air Force at Barksdale AFB, Shreveport, Louisiana. He also served as the Chief of the Strategy Plans Team in the CENTAF CAOC. In December 2006, Colonel Jensen was selected to command the 343d Reconnaissance Squadron, Offutt AFB. He also served as the commander of the 763d Expeditionary Reconnaissance Squadron and the deputy commander for the 55<sup>th</sup> Operations Group and 404<sup>th</sup> Air Expeditionary Group, Ramstein AB. Colonel Jensen is a Master Navigator with over 3,500 flying hours.

## **A Corrupted iCon: A Life Lost in 2035**

*Walking briskly from the Global Neuroware Kiosk, Eve smiled up at the warm sun and excitedly inhaled the precisely maintained 72.1°F fresh Montana air. Eve loved the temperature her conurbation had almost unanimously chosen during the winter climate balloting. She quickly blinked her eyes to the upper left quadrant of her vision grid to signal her iNeu implant that she wanted to establish connection with her boyfriend. She had big news to tell.*

*“Hello?,” came an inquisitive voice over Eve’s iNeu.*

*Eve chided Hal. “Hello? Is that any way to greet your dream girl?”*

*Then came a long, awkward pause. “Um, who is this? I don’t see your data stream,” said the voice on the other end.*

*“Hal, this is Eve. Stop messing with me; I have my new app from Global. I can change my eye color now to whatever you want. Won’t that be fun?”*

*“I’m sorry; I can’t confirm you for some reason. Please send me your DNA” (Data-Neuro-Avatar).*

*Eve slowed her pace and then stopped. Eve was used to Hal’s dry sense of humor and constant pranks, but his voice and the emoticons piped in from his iNeu indicated he was genuinely unsure of who he was talking to.*

*“Hal, this is your girlfriend, Eve. We’ve been dating six months you big silly. Here’s my DNA, as if you don’t already have it as your favicon.”*

*Eve went through the motions of accessing her DNA through her iNeu visual reference system displayed on her pupils, but the file was empty. She double checked and then went to her back-up server. Nothing.*

*“Um, Hal. I don’t know what to say, but I seem to have lost my DNA. My iCon must be corrupted.”*

*Hal didn’t know whether to feel sympathetic or skeptical. Was this really Eve or was this a hacker looking for another target?*

*“Eve? Look, I want to believe you, but you need your iConscience restored ... unless someone completely corrupted you. I’ve seen bits on this recently; seems to be on the rise. Try this. Disconnect from me and contact your iCon provider; maybe they can reinstall your DNA.”*

*Eve stood motionless, letting the realization sink in that she’d been hacked. As far as the world was concerned, she didn’t exist.*

## Introduction

*“... you must not eat from the tree of the knowledge of good and evil ...”*

*- God (Genesis 2:17)<sup>1</sup>*

### ***Brave New World of Cyberspace Threats and Deterrence<sup>2</sup>***

How does one prevent someone from doing something they do not want them to do?

Although the opening quote from the Bible indicates this question is as old as humankind, people continue to seek viable solutions to the problem of deterring objectionable behavior. This universal search for a solution spans the full spectrum of human relationships from one-on-one parenting in homes to nation-to-nation international relations at the United Nations. Possible solutions to this timeless question, within the context of national security studies, are posed in deterrence theory.<sup>3</sup> Reflecting a renewed emphasis on answering this question, the Department of Defense (DoD) is examining “evolving theories of deterrence.”<sup>4</sup>

By reexamining long-held beliefs on deterrence, the DoD is seeking new ideas in the wake of “technological breakthroughs and shifts in the geostrategic environment (which) can dramatically affect deterrence theory and potentially render aspects of it obsolete.”<sup>5</sup> This timely research objective can be applied to many areas of national security, particularly in the contested and constantly evolving cyberspace domain. With such rapid advances in cyberspace technology, the DoD seeks to understand how nation-states manage the risk of escalation as other nations and non-state actors acquire increasingly lethal and sophisticated capabilities in this domain.

Specifically regarding non-state actors, the DoD is highly concerned with managing risks perpetrated by cyber-savvy individuals due to the unexpected and unpredictable nature of this potentially catastrophic threat. In fact, a single individual will, by design or miscalculation, have

the ability to dissuade, disrupt, deny, degrade and destroy via cyberspace.<sup>6</sup> Deterring this behavior will require the deterring nation to develop new ways to ferret out and identify individuals whose intent is doing harm. Finding such a person in the increasingly nebulous world of cyberspace will require new methods, tools, skill sets, and technologies which, when combined, provide a cumulative level of insight that is akin to omniscience.<sup>7</sup>

The terms cyberspace and omniscience will be fully explored later; however, brief explanations are needed. *Cyberspace* is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”<sup>8</sup> *Omniscience*, within the cyberspace realm, is the ability to conduct comprehensive intelligence collection on any [potentially] threatening cyberspace activity followed by near-simultaneous processing, exploiting and disseminating of the information. In essence, cyberspace omniscience is Intelligence, Surveillance, and Reconnaissance (ISR) in the cyberspace domain. Paired with cyberspace, ISR is the requisite ability to identify, track and prosecute the offender.<sup>9</sup> A full examination of this concept along with definitions follows below; it is important to note that this concept is best understood in the technological and societal environment that could emerge by 2035.

### **Purpose and Research Methodology**

Developing a theory of deterrence requires postulating about the nature of a battlespace, making assumptions about actors, their means and motivations, and then posing possible deterrent solutions to discourage the objectionable behavior.<sup>10</sup> This paper will begin the process of developing the theory of cyber omniscience as a DoD deterrent. At the heart of cyber deterrence lays this question: “As technology rapidly advances in the contested cyber domain,

can hostile individuals be deterred from employing highly advanced technologies through cyberspace that threaten national survival?” To answer this question, this paper will investigate a number of issues with regard to cyberspace deterrence: anticipated life (societal norms) and technology in 2035, hostile individual threats, what cyber omniscience entails, privacy issues, and policy recommendations. This multi-pronged approach will serve as the catalyst to a better understanding of the future of cyberspace, the threats, and deterrence.

### **Definitions and Explanations**

Before exploring what life and cyberspace will be like in 2035, there are several key terms that must be defined. Some terms are created by the author for this paper, while others are defined via academic sources. A few terms are used only in the vignette while others are used throughout the paper. Collectively, they help frame the future environment for cyberspace deterrence.

iCon is an amalgamation of three terms. The first is from the Greek word *eikōn* or “image” which, in a broad sense, represents a picture or likeness of an individual.<sup>11</sup> An icon is a pictogram used to represent a function; a pictorial shortcut.<sup>12</sup> As used in the opening vignette, iCon is an abbreviation for iConscience which captures the idea of a human-technology merger that produces physical and virtual self awareness; all conscious connections, thoughts, and information about a person can be captured, stored or accessed in a manner similar to a computer file. In short, iCon is a person’s consciousness in cyberspace.

DNA is an acronym for Data-Neuro-Avatar. This created term intentionally mirrors Deoxyribonucleic Acid (DNA) with the idea that all that is knowable about a person is captured in our DNA – both biologically and technologically. DNA, in the context of this paper and in 2035, represents our entire “body” of data for a person while iCon represents our “mind.”

iNeu is a created slang term for the word iNeuro. In the vignette, the iNeu is an implanted device which provides constant personal, direct access to cyberspace. Similar in concept to the cellular phone ear buds we see today, iNeu users constantly transmit and receive information for enhanced awareness.<sup>13</sup> Unlike the ear bud, this personal communications device is surgically implanted and acts as the physical device which connects an individual's iCon and DNA to cyberspace.

Omniscience is infinite, total knowledge.<sup>14</sup> It is the ability to know and understand everything there is to know at the instant it can be known. To put the term in context, omniscience is a characteristic most often ascribed to God. Although omniscience is not considered humanly attainable, this essay has intentionally, but cautiously, used the term in the first half of the title to emphasize the comprehensive nature and context of cyberspace in 2035.

Cyber, cyberspace and cyber domain are used interchangeably in this paper. The definition provided earlier from Joint doctrine will be an incomplete description of the expansive cyber environment of 2035. Due to expected growth in capability and use of technology, it may be difficult to distinguish boundaries between cyberspace and *all* associated technologies.<sup>15</sup> In fact, it is essential for the reader to imagine a boundless world of comprehensive connectedness in and through cyberspace. In a similar manner in which all humans are "connected" to the surface of the Earth (where every human is on the same surface, just a few feet or several thousands of miles apart), so too humans can be connected to nearly any other human or information on Earth via cyberspace.

Combining these last two terms, cyber omniscience is based on the idea that nearly all important human interactions in cyberspace can be known and monitored. This monitoring can be active or passive, and could include any use of the Internet (commerce, banking, email,

blogging, reading, posting, hosting, Voice Over Internet Protocol, etc.); all telecommunications (both directly and indirectly monitored conversations, texting, data transfer, etc.); tracking the location of any Global Positioning System (GPS) device; monitoring all video systems (web cams, public surveillance, computer/cellular phone cameras, clandestine placements, any device that can capture video and is connected to cyberspace); surveillance of what people read (via Kindle-type readers as well as purchases); all electronic commercial transactions (supermarket, internet purchases, etc.); and medical monitoring (via hospital databases, smart clothing and smart homes).<sup>16</sup> We already see examples of this in 2010 in military, federal, and civilian intelligence collection practices. Common examples used today are satellites, Internet monitoring, network mapping, web cameras, social networking software, and advanced signals intelligence. Although it is important to understand the full suite of actual and potential capabilities, it is essential to highlight the limits of cyber omniscience.

The term “*toward*” in the title of this paper is used to convey two thoughts. First, this deterrent capability will continue to evolve along with cyberspace technology and its myriad of uses. In the same way that modern intelligence collection has progressed from using a spyglass to satellites for monitoring enemy activity, the ability to conduct surveillance in the cyber domain will also evolve in terms of technology and how it is used. Thus, it is probable that cyber omniscience will always be a journey rather than a fixed destination. Secondly, complete cyber omniscience is unachievable, at least by 2035, because the threat is a *maneuvering adversary*; an intelligent individual who will strive to find a way to either circumvent or thwart technologies, tactics, techniques, and procedures associated with cyber omniscience. The desired end state is to maintain the advantage in omniscience sufficient to deter the hostile nation-state, group, and individual.<sup>17</sup>

Transparency carries two definitions, depending on context. First, transparency can apply to something that is occurring without user knowledge. For example, it is transparent to a user that a cellular phone transmits its location to the service provider. The user neither directs it, nor knows their position can be tracked over the Internet.<sup>18</sup> Secondly, transparency can apply to the relatively easy accessibility of information about individuals, their family and friends, the company they work for, or nearly any other data affiliated with the individual.<sup>19</sup> In 2035, most personal information will be readily available through an individual's iNeu-like implant which may create a near-constant communication and learning mode. Picture an environment where curiosity and wonderment are satisfied by knowledge automatically pushed to users. Some established futurists believe this rapid technological change and human dependence upon technology are converging to a state of being known as the *Singularity*.<sup>20</sup>

According to Ray Kurzweil, *Singularity* is, "a future period during which the pace of technological change will be so rapid, its impact so deep, that human life will be irreversibly transformed."<sup>21</sup> Kurzweil envisions a time beyond 2045, when it will be difficult to distinguish between human and non-human; where technology and people are wedded through cyber implants resulting in a complete transcendence of humans and technology. Nearly all aspects of humankind and the human experience will be replicated, replaced or enhanced by technology.<sup>22</sup> While Kurzweil's *Singularity* reaches beyond the timeframe explored in this paper, many notable precursors will pave the way for a near-transcendent life in 2035.

## **The Convergence of People and Technology in 2035**

### **Is It Live ... Or Is It the *Singularity*?**

One of the most iconic television commercials of the 1970's was aired by the cassette tape company Memorex. In the commercial, Ella Fitzgerald breaks a wine glass by striking a

high pitch at the conclusion of a song.<sup>23</sup> While the viewer is asked to discern if Ella or the recording actually broke the glass, the implied answer is that either may have done so. The underlying message is that consumers (and wine glasses) cannot distinguish between live and recorded sound. Perhaps this is one of the earliest commercial steps toward *Singularity*: the inability to distinguish between people and technology. This commercial, combined with the opening vignette and the definitions above, illustrates the anticipated integration of people and technology in everyday life. A further examination of people and technology will help explain what is required of each on the path toward cyber omniscience.

Capable technology and continued societal change are fundamental elements of cyber omniscience. They represent a convergence of developments – exponential technological advances that make *Singularity* possible and the forces at work in a society where people readily adopt these advances. What technologies are possible by 2035?

Joel Garreau wrote a captivating book called *Radical Evolution* whose title refers to the next extraordinary phase in human development in which people will become increasingly enhanced with technology.<sup>24</sup> Integral to this phase are four interrelated technologies which he calls GRIN: genetic, robotic, information and nanotechnology processes.<sup>25</sup> A brief description explanation of each will prove helpful.

The GRIN technologies help bridge the divide between human and non-human. The first part, genetics, speaks to the advances scientists are making in the understanding, manipulation, and fabrication of the human genetic code. On the horizon is a time when human DNA will be open to modification and enhancement.<sup>26</sup>

The second area, robots, has long since passed the science fiction phase and is nearing ubiquitous status on the battlefield, in the factory and home, and in many public sectors<sup>27</sup>. These

robots in *Radical Evolution* gain their significance when paired with the fourth area, nanotechnology. Nanotechnology is more than simply fabricating extraordinarily small substances. Nanotechnology promises to deliver autonomous machines, self-replicating devices and new materials which will exist within other technology or even *living systems*.<sup>28</sup> This capability opens the door to the development of entirely new options and enhancements for people, animals, and machines.<sup>29</sup>

The third requirement, information, has become an overused and almost benign term in modern society. In the context of GRIN, *Singularity*, and *Radical Evolution*, information is the lifeblood of awareness, instruction, command and control, and organization. By contrast, virtually any form of technology that manages to exist without information is essentially “dead.” Additionally, all four GRIN technologies need to be viewed in an interdependent context where one or more enable the others to act as technology force multipliers. Note there are and will be many additional technologies that are supporting, supported and parallel to GRIN; these four combine to form the cornerstone of *Singularity* due to their capability to bridge the human-to-technology gap. Garreau then takes the GRIN technologies a step further by pairing them with three hypotheses which emphasize their impact on a future fueled by rapidly advancing technology.

Garreau believes GRIN serves as the enabler for three hypotheses which are working together to create the environment for *Singularity* to emerge. They are (1) the curve of exponential change, (2) this change is unprecedented in human history, and (3) it is transforming human nature.<sup>30</sup> When viewed in isolation, there may not appear to be anything remarkable about these hypotheses. When one considers, as Garreau and Kurzweil do, that the world is approaching a convergence which will combine GRIN and the three hypotheses, it becomes

readily apparent that people and technology will be interdependent, and sometimes, indistinguishable. To assist his readers in imagining these conclusions, Garreau created three alternate futures: Heaven, Hell, and Prevail.<sup>31</sup>

The three scenarios help futurists and philosophers envision a trail blazed by GRIN and the supporting technologies. Although the names Heaven and Hell may self describe, it is important to note that subscribers to these beliefs imagine these scenarios as unfolding *with little or no control from humans*. In other words, unprecedented technological change is transformative making it virtually impossible for people to stop the Heaven or Hell scenario from developing. Effectively, they will take on a life of their own (figuratively and literally) as the development and use of these technologies enter society.<sup>32</sup> Contrasting the polar technological opposites of Heaven and Hell, the Prevail scenario allows for and expects humans to be in control, thus avoiding a technological “run-away train.” The Prevail scenario is uncertain and non-specific because it is unclear who will be in charge and how far humans will allow technology to progress.<sup>33</sup> Garreau cites some examples to illustrate the types of scenarios that may play out in Heaven and Hell:

#### Heaven Scenario<sup>34</sup>

- Direct connections between the human brain and machines will transform work in factories, control automobiles, ensure military superiority
- Wearable sensors will enhance every person’s awareness of his or her health condition, environment, chemical pollutants, potential hazards, and information of interest about local business, natural resources, and the like
- The human body will be more durable, healthy, energetic, easier to repair, and resistant to many kinds of stress, biological threats, and aging process

#### Hell Scenario<sup>35</sup>

- Destruction of all or part of the human race

- Enhanced humans subjugating fully natural (unenhanced) humans
- Human nature reduced to machinelike soullessness<sup>36</sup>

These two scenarios are in conflict with each other, but they do agree this is potentially where technology will take us; neither is preordained. These two sample sets, along with Prevail, help manage expectations as to what our future may look like. Some practical examples from today's emerging technology are worth considering.

Some technological indicators of the emerging future include the already demonstrated capability for smart clothing that will provide medical assessments, location and physical performance enhancements.<sup>37</sup> Smart homes exist that can automatically sense and protect themselves from severe weather while also generating their own energy resources.<sup>38</sup> Bringing revolutionary meaning to the term social networking, cellular phones will likely be replaced with cochlear, oral and optical implants that will allow people to record, share and view every aspect of their lives while sharing in the life experiences of anyone socially networked.<sup>39</sup> For example, an individual may be able to share a scent or taste with someone via an iNeu-like system. This person could either be sitting next to you or connected with you from another country. Flowing through all this technology will be terabytes of information which will create an environment rich with comprehensive solutions shared via this new transparency. To progress from GRIN and *Singularity* to this future reality requires an examination of people and their role in this emerging transparent environment.

### **Two Shall Become One: The Marriage of People and Technology<sup>40</sup>**

History is sometimes a keen predictor of the future. One need only look to the past to see that humans tend to respond in a predictable manner to certain situations. Within the context of technology, "people have a tendency to transform, and even subvert, the intentions of designers

in order to manifest social capabilities in their tools.”<sup>41</sup> In other words, when people are presented with a new tool (fire, wheel, gunpowder, silicon chip, Internet, cellular phone), they tend to adopt the technology as well as make the technology adapt to other uses. The history of the origin and growth of the Internet provides an ideal technological example.

The Internet’s precursor, ARPANET (Advanced Research Projects Agency Network), launched in 1969, was served a scientific purpose of sharing information and computer resources.<sup>42</sup> Here, the professors and students adopted the technology in order to improve their research. In time, through technology advancements and increased access, the “tool” morphed into the Internet. What was originally a vehicle for scientific data transfer in 1969 became a catalyst for the Information Age and a social revolution through the explosion of e-business, on-line education, information access and social networking.<sup>43</sup> All of these areas grew out of adapting basic technology for other uses. The Internet went from being “created,” to people using it to “create” countless other uses. Another example of adoption and adaption is personal communication devices.

The earliest cellular phones were huge “bricks” with a revolutionary feature ... a telephone with no wire. Today, virtually everyone in both modern and developing societies has or can access wireless communications. Adding to basic voice communications is the option to send and receive electronic mail, textual (text) messages, and visual data such as photos or videos. Unlike the adoption of the Internet, which took many years to reach the common market, cellular phones and personal electronic devices have been adopted at an extraordinarily rapid pace.<sup>44</sup> Some countries, such as India, Nigeria, and Afghanistan, which never had wide-spread land-line telephone service, have hurdled intermediate steps to establish nearly nation-wide cellular telephone use.<sup>45</sup> This behavior shows that people can rapidly and comprehensively adapt

to new technology. These new uses of technology meet critical communication needs, but there are more personal aspirations for technology, especially in the medical realm.

### **Was Blind, But Now I See<sup>46</sup>**

Barbara Campbell was not born blind; she began losing her sight as a teenager and was legally blind by the time she was an adult living in New York City. What makes Barbara special is she has “bionic eyes.”<sup>47</sup> She was diagnosed with retinitis pigmentosa, a progressive degenerative disease which damages the part of the eye that detects light. Her new remedy, in scientific terms, is an artificial retina containing microchip implants composed of tiny electrodes with wires connected to the sight receptors in her brain. Although her vision is not completely restored through this experimental program, she is able to see light for the first time in years. In a recent test, she was also able to correctly identify a row of letters. This is one of the many examples of advancements in medical technology demonstrating the potential for human enhancement as well as society’s willingness to adapt technology to new and extraordinary applications.

By the year 2035, it appears the convergence of technological advances and a historically adaptive society will create conditions for *Singularity* and cyber omniscience to emerge. Although society can anticipate numerous positive improvements in their daily lives as a result of these changes, they may also face new and more threatening vulnerabilities from individuals operating in cyberspace.

## **The Cyber Threat: The Hostile Individual**

### **David and Goliath: The Small versus the Great**

The individual threat is perhaps the most challenging hazard to the DoD because of two key components: size and time. The cyber individual is the proverbial needle in the cyberspace

haystack; a particularly cyber-savvy individual will be able to study, infiltrate and exploit a cyber system with little risk of detection. Adding to the complexity of this threat, an individual, unlike a nation state or group, does not necessarily have a specific timeline, a supervisor, rules of engagement, or boundaries. Also adding to the power of the individual is the idea that eventually one of the most important principles of war, mass, will no longer require large numbers of people, or in this case, hackers, to launch large scale attacks.<sup>48</sup> A single individual using advanced packets of programming, may single-handedly seize millions of computers, including cyber enhanced people, and employ them in much the same way Napoleon used “mass” to conquer Europe. This new cyber mass will be involuntarily co-opted by malicious programming and employed with devastating effect in and through cyberspace.<sup>49</sup> Complicating this threat is the dimension of time.

### **Time Is Not On Our Side**

A little observed consideration for cyberspace vulnerabilities is time. Unlike human combatants who have to wait for moonless nights or calm seas, individuals can choose any time to attack. This requires the DoD to be on “full alert” at all times and in all areas of the domain. Also nested in this wide-ranging, unblinking threat is time itself. All of cyberspace runs on the same time regardless of location, languages, duty hours, or weather. Atomic clocks in the Global Positioning System Satellite Operations Center outside Colorado Springs, Colorado provide the timing necessary to synchronize the programming satellites, servers, and support systems -- they serve as the mechanical heartbeat of the global cyber system.<sup>50</sup> This is important because it effectively facilitates the attacking software to march to a synchronizing cadence across the planet and the entire cyberspace domain. Individuals are not only small and can mass effects, but also are a thinking, deceptive threat.

## **Toward Cyber Omniscience: Deterring the Individual in 2035**

### **Videmus Omnia**

How do people behave when they know someone is watching them? Generally, many people behave awkwardly or at least differently because the observer makes the observed more self conscious about what they are doing. That said, most members of society are living their normal productive lives and either are unaware or do not care that they are being monitored by traffic cameras, financial systems, cellular phone towers, email scanners, video security systems or satellites. Generally speaking, they have nothing to hide and have grown accustomed to public surveillance.<sup>51</sup> By contrast, individuals with malevolent intent do their best to remain undetected by authorities. They will use identity theft, forgery, Internet Protocol spoofing, and counterfeiting to hide their identity and efforts in cyberspace. Additionally, these individuals will deceive, disable or destroy monitoring equipment to allow them to proceed to their intended target unobserved. In a future environment where all cyber activity is observable, cyber omniscience could counter this malevolent behavior.

The motto of the 55<sup>th</sup> Wing at Offutt Air Force Base is “Videmus Omnia,” which roughly translates from Latin to: “We See All.”<sup>52</sup> This Air Force wing is home to many airborne intelligence, surveillance and reconnaissance platforms that collect various types of intelligence from a wide variety of sources in order to provide near-real time information to national security decision makers. In a similar manner, through cyber omniscience, the DoD will be able to sense and collect information from a wide variety of cyber systems, and work to provide a picture of activity that is threatening to the United States. But how does this movement “toward cyber omniscience” deter an individual?

As the DoD moves toward cyber omniscience, it must develop a “system of systems” that is capable of monitoring the massive, ever evolving and progressively more amorphous cyberspace architecture. This system will monitor all cyber activity, discern trends, and define connections between information and people.<sup>53</sup> It will be able to see, hear, and sense threatening behavior through passive collection and data-mining across cyberspace. The all-seeing cyber search engine will look for key words, activities and patterns that may indicate threatening behavior. The system envisioned will run quietly and unnoticed in the background of cyberspace with little to no human interaction until an anomaly is detected that threatens to compromise the established data protocols for legal use of the domain.

A recent demonstration of this data-fusion was conducted by Palantir Technologies in Palo Alto, California. This Silicon Valley company “designed what many intelligence analysts say is the most effective tool to date to investigate terrorist networks.”<sup>54</sup> What sets Palantir apart is, “a user-friendly search tool that can scan multiple data sources at once, something previous search tools couldn’t do.”<sup>55</sup> Through this search architecture, Palantir is discovering connections between actors and actions – a key dimension of cyber omniscience.

Once an individual of interest has been identified, depending on the type and intensity of their objectionable behavior, additional levels of monitoring will be activated automatically in order to build a fuller picture of the individual’s behavior. This deeper search will take the form of video surveillance (by leveraging local options, overhead or even the individual’s own computer camera), monitored phone calls and financial transactions, and searched emails/Internet activity -- all without him or her knowing they are being monitored. The key is the automatic transition from a passive to active monitoring search algorithm. If this active monitoring identifies threatening behavior, the cyber omniscient system will alert law

enforcement personnel to intervene in the assessment to determine the appropriate course of action. Of note, by the time people are brought into the investigation, cyber omniscience will conclusively identify a hostile individual or a person of interest.

A person of interest may be innocent or may be someone actively concealing their cyber activity. The objective of this classification is to address those individuals who require additional monitoring until a conclusive assessment is completed. The nature of any investigation will depend on the degree to which it affects national security; in some grave circumstances, the system would self-identify and initiate preemptive action. If appropriate, the system would automatically provide scalable options to isolate the individual and block further actions.

To expand on the “non-human” aspect of cyber omniscience, it is important to understand that the primary intent of this system is not to autonomously identify, track and prosecute an individual without human intervention. As we approach *Singularity* in 2035, cyber omniscience, under extraordinary circumstance, may need to act preemptively in an extremely rapid manner. As such, there may be instances where the response capability cannot wait for human intervention. In these cases, threatening individuals are in no way harmed, they are simply isolated from cyberspace. The responding law enforcement personnel can investigate and, if necessary, apprehend the individual. As a simple example of this concept, police recently apprehended a car thief by using General Motors’ On Star system. The service remotely disabled the gas pedal and the vehicle came to a stop. The thief was apprehended when he attempted to flee on foot.<sup>56</sup> If not now, in twenty-five years, an automobile (which is connected to cyberspace via GPS, cellular phone, satellite radio, and system monitoring) will be another cyberspace node.

## **Calculus Of The Criminal Mind: Does the Benefit Outweigh the Risk?**

According to Joint doctrine, deterrence is “the prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.”<sup>57</sup> Ultimately deterrence is about having a psychological impact on the individual who seeks to do harm to the one who is posturing the deterrence. The result is altered behavior by the individual. A successful DoD deterrent must be both *capable* and *credible* – a weapon system that can perform as advertised, is a significant threat, and whose use is plausible.<sup>58</sup> Deterrence may be in the form of dissuasion, denial, and threat; all three have a place in cyber omniscience.<sup>59</sup>

Deterrence by dissuasion in cyber omniscience involves advertising the ability to positively identify and attribute actions to individuals and then thoroughly monitoring any suspicious activity, no matter how seemingly benign. Omniscience capabilities must be made public so individuals are forced to conduct a cost-benefit analysis and determine acceptable risk. The risk of being caught will affect their decision to act.

Deterrence also relies on denial; defending the domain from individuals who cannot be dissuaded. Cyber omniscience would allow swift identification of individuals, characterization of the threat they pose, and then aggressive defense of DoD’s cyberspace realm. What sets this type of defense apart from today’s security measures is the speed and completeness with which threats are identified and prosecuted. For example, cyber omniscience would allow systems to keep a selected target list of people and locations of threatening behavior. As a Hostile spends more time in cyberspace, cyber omniscience would observe behavior and note patterns. Through observation, it develops a better understanding of certain individuals, enhances its sense of who may pose the greatest risk, and who warrants closer scrutiny. As threats manifest themselves,

rapid reaction and system denial would act as a significant deterrent to hostile individuals seeking to exploit DoD's cyberspace domain.

The final area of cyber deterrence involves the capability and credibility of DoD's response (threat). Anyone who considers committing a crime tempers their behavior based on the risk; on whether they think they will be caught, and how severe the punishment might be. For Hostiles in 2035, the punishment may no longer entail physical incarceration methods. Instead, criminals may be barred from connecting to cyberspace. The DoD, using cyber omniscience and its selected target list, would be able to monitor and bar access to criminals for any set amount of time. In other words, they would be kept out of cyberspace. This virtual form of banishment is somewhat akin to the practices used by medieval kings when they banished noblemen from their court until the king felt they had been appropriately punished.<sup>60</sup> For the most serious cases affecting national security, cyber *capital punishment* may be warranted. An individual may find their iCon permanently deleted and they no longer have the ability to connect to or use cyberspace. While capital punishment implies deterrence has failed, the deterrent value of a cyber execution (or excommunication) will be an unbearable "cost" to many. Such thoughts echo similar themes from George Orwell's *1984*.

### **Is This 2035 ... Or 1984?**

#### **Big Brother is Watching You<sup>61</sup>**

Any reference to George Orwell's classic dystopian novel, *1984*, conjures up vivid images of an extreme totalitarian regime that criminalizes free thought and human emotion. Could cyber omniscience be a vehicle for enabling Orwell's vision in 2035? The concept of cyber omniscience indeed prompts concerns about privacy, personal security, constitutionality, and the potential for Orwellian oppression.<sup>62</sup>

In 1984, the main character, Winston Smith, works for the Ministry of Truth as a “civil servant responsible for perpetuating the Party’s propaganda by revising historical records to render the Party omniscient and always correct, yet his meager existence disillusioned him into rebellion against Big Brother, which leads to his arrest, torture, and conversion.”<sup>63</sup> One of the central slogans the totalitarian party uses is “Big Brother Is Watching You.”<sup>64</sup> The mixed message is that someone is looking out for a person like a big brother would, but it is also clear that every thought, action, and spoken word is monitored for compliance with the norms established and regulated by the state. How would cyber omniscience be different?

The theory behind cyber omniscience is not one of direct control, enforced correctness or even mandated compliance. It is specifically centered on and used for deterring aggression in cyberspace; by design, deterrence allows an aggressor to make a choice. The intent, as with all DoD deterrence strategies, is to prevent malevolent behavior from maturing into a national security threat. In Orwell’s account, *Big Brother* monitored its people to ensure compliance with Party orthodoxy while cyber omniscience seeks to prevent attacks against the nation. In fact, cyber omniscience would work to prevent someone from using cyberspace as a *Big Brother* might because such behavior would invite increased scrutiny. For example, if a Hostile uses cyberspace to monitor the location and behavior of, and then attempt to influence, of key individuals, cyber omniscience would identify this as suspicious behavior. Tailored monitoring would allow decision makers to respond appropriately and then deny those engaged in the malicious behavior any opportunity to gain an advantage.

### **“I’m From the Government and I’m Here to Help”: Privacy Versus Security**

The natural tension between privacy and security has always been an issue between those who value privacy over security versus those who see a threat behind every computer. Within

cyberspace, the struggle between privacy and security will perhaps always be with us.

Ironically, cyber omniscience may actually address both concerns.

The core competency of cyber omniscience is manifested in an array of human-less data bases and super computers that do not “care” who an individual is, what they think or believe, or what their social life is, until malicious intent and malevolent behaviors surface.<sup>65</sup> One way to understand the underlying theory of executing cyber omniscience is found in traffic cameras.

Traffic cameras omnisciently see all vehicles passing through intersections, collecting snapshots of license plates, and, possibly, the driver’s face; they are triggered only when a person violates traffic regulations by speeding through an intersection after the light has turned red. None of the information collected is relevant or revealed until someone runs a light or *in extremis*, evades capture by police. Those who may consider running a red light are warned by signs prominently placed before the intersections that cameras are monitoring their actions and are used to enforce traffic laws.<sup>66</sup> This form of dissuasion allows the individual to make a choice about their actions. If they choose to violate the law, the data collection and traffic enforcement mechanisms become operative in the deterrence calculus. The license plate can be associated to the registration, driver’s license, social security number, and home address of the alleged offender. The police also use this information to check for outstanding bench warrants and unpaid parking tickets.<sup>67</sup> This is a simple, but revealing example of how cyber omniscience would unobtrusively work in the background until a Hostile violates the law in cyberspace. Although many are concerned about privacy, these fears may not be universal.

An emerging development with cyberspace and younger generations (early teen to mid-twenties) is they may have a different privacy standard. For the generations that have always had cell phones, the Internet, Facebook, Twitter, and other public cyber venues, privacy is

simply limited to those things that the individual has *not* disclosed about themselves – not necessarily what is already knowable about them. In the same way that this generation largely expects information to be readily available and free, they also expect their lives will be known by others using cyberspace.<sup>68</sup> What will future generations consider private? It depends; Facebook and other social network sites today allow individuals to provide as little or as much personal information within bounds of propriety established by the Terms of Use agreement between the individual and the service provider. Some of the information shared is often extensive and deeply personal; some individuals appear to have little concern about the damage done to personal reputation. The connection to cyber omniscience in society may shift to a more liberal view of privacy.

Regardless of where one falls on the privacy-versus-security spectrum, it is doubtful society as a whole will agree on what constitutes reasonable standards of privacy when balanced with deterring threats. The United States government must codify its position via policy statements to the public, other countries, and potential hostile individuals as to how the DoD will deter aggression in cyberspace.

## **Policy Recommendations: Getting Ahead of the Future**

### **Cyber Deterrence Policy Options**

The future always arrives whether one is prepared for it or not. Therefore, the DoD must take a proactive stance today to deter threats in what is already a contested domain. A lag in deterrence policy potentially yields all or part of the domain to individuals who threaten our national security interests.<sup>69</sup> In response to these concerns, this section will consider policy factors and recommend options.

The research for *Toward Cyber Omniscience* uncovered no less than two dozen policy options covering a variety of cyberspace areas. These options included restructuring the United States Government and DoD to better meet the needs of cyber control and threat defense while other policy measures focused on current security methods such as firewalls, trust and authentication.<sup>70</sup> These are all important, but do not directly address future needs in a world of exponential technological change. With cyber omniscience as a possible end state, this paper will focus on access, international agreement, privacy, and cyber law.

The DoD will need complete access to, and freedom to maneuver within every area of cyberspace if omniscience is to be both capable and credible. The strength of cyber deterrence is its omniscience; there can be no blind spots or ungoverned areas of cyberspace. To achieve this capability, government policy must guarantee access to all domains, businesses, Internet governing authorities, administrators, universities, hosts, servers, sites, etc. Those with little knowledge about cyber omniscience may not fully understand its role or how cyber omniscience operates. With its neutral status as a passive monitor, it will neither collect nor store sensitive material, trade secrets, corporate strategies or personal information that is not relevant to dissuading, denying or threatening a Hostile. In 2010, this is a difficult concept to accept. It is also difficult to envision how neutral this monitoring will be, so omniscience policy must make clear the need for access and the non-voyeuristic nature of the monitoring.

International agreement is a necessary enabler for full access to all areas of cyberspace. Every country with significant cyberspace capabilities fears hostile individuals, but may also doubt the intent of the United States government as it protects its national security interests in cyberspace. Although it is doubtful other countries will allow full access, even if it is mutually beneficial, all must work toward finding common ground on this contested battlefield. Policies

sponsored by the United Nations or a specific cyberspace international governing authority could provide a forum for countries to share information about cyber Hostiles and also help establish a common legal framework for prosecuting offenders. Additionally, international policy could mirror current agreements that either bar travel to another country or allow extradition of cyber criminals. In the cyberspace realm, a person does not need to physically travel to enter another country's *cyber borders*, so the international policy must recognize this non-traditional, invisible boundary.

As previously addressed, privacy will be the chief concern for nearly every cyberspace user. Concerns about a 1984-style totalitarian state aside, Americans value their privacy and free speech rights. As the DoD moves toward using cyber omniscience as a deterrent, strict policies must prohibit illegal use; protocols must be a part of the fabric of the technology which will prevent it from being misused. While cyber omniscience can detect and neutralize threatening use in the same way it detects illicit misuse, it is also important to remember that the system would be designed to primarily operate independent of human interaction. This does not mean humans cede all power to "the machine" which lacks empathy and human judgment. Instead, this lack of human interaction provides a privacy shield for everyone. The United States Government has a long-established history of attempting to balance the needs of the few with the needs of the many. Similarly, privacy for all must be balanced with security for all.<sup>71</sup>

Cyber law is the final policy area that needs significant development. By contrast to this emerging area of jurisprudence, maritime law is steeped in thousands of years of history and countless case studies and legal decisions. Lacking this level of understanding and tradition, cyber law is still in its infancy both in America and internationally.<sup>72</sup> Ironically, this rapidly developing domain may need more law and policy governance because it does not have the

benefit of tradition and established norms. Criminals have always gravitated toward those places that are ungoverned and unprotected, so unless the United States authors, sponsors, and campaigns for new and relevant laws, the contested cyberspace domain will always be readily accessible by Hostiles.

These policies are simple, yet depart from the current conventional wisdom because of the projected timeline of this paper and the controversial nature of this deterrent theory. In order for cyber omniscience to reach maturity in time to deter hostile threats in 2035, policy makers must establish policy which grants access, networks with international bodies, balances privacy with security and is codified in both United States and International law.

## **Conclusion**

### **Cyber Salvation**

*Eve disconnected from Hal and took a moment to collect her thoughts. Was this just a technical glitch resulting from the newly installed app? Or was something more sinister at play? The more she thought about her lost iCon and digital amnesia, the more anxious she became.*

*She quickly looked at the help prompt in the bottom left corner of the visual grid and blinked to connect to the Omnia Cyber Help Center.*

*A cheerful voice piped into Eve's ears from seemingly two feet away, "Omnia Ops, how may I help you?"*

*"Um, hi. This is Eve Zuse. I think I've been hacked or had a bad app install. I can't access my iCon, my DNA is gone ... and I'm really freaking out." Eve was shaking uncontrollably and could barely stand. She moved over to a nearby bench and sat down.*

*"Yes, Eve, we know. Omnia is tracking your hacker and have dispatched an interception team as we speak. Omnia had some initial indication two days ago, but lost him when you went to Global for your download. We suspect he hit you while you were offline for the app install."*

*"Wow, um, thank you. What do I do now?"*

*"Your iCon is coming to you now ... see it?"*

*“Well, I can hear it.”*

*“Same thing. That’s a good sign. Can’t help you with recovering the new app since we didn’t have you on the grid after the install. See Neuroware about that.*

*“That’s ok, I think I like my eyes just the way they are.”*

*“Uh, yes, ma’am. Omnia Ops out.”*

### ***This Land Is Your Land, This Land Is My Land – Why Cyber Omniscience Matters***<sup>73</sup>

In Woody Guthrie’s classic folk song, he describes a blessed America of vast lands, highways, and skyways with a rich collection of natural resources. In a nearly identical manner, in 2035, “our land” will be cyberspace. We need to view it as a place of rich information resources that must be valued, protected, and governed. From a DoD perspective, sovereignty of the cyber domain must be viewed on the same level as territorial sovereignty which requires a vigilant defense.

So again we ask, “How does one prevent someone from doing something they do not want them to do?” This still is, and always will be, a challenging question. Unfortunately, as we approach the year 2035, the severity of malicious behavior in cyberspace will increase significantly. With near-complete connectedness and absolute dependence on cyberspace, one can only imagine how hostile individuals will exploit others in this contested domain. There is more at stake here than mere ones and zeros.

As *Singularity* approaches and transparency becomes the coin of the realm, cyberspace will be no different than one’s homeland, their personal thoughts, and their very lives. It will be “our land” because it will be a part of the individual in a very real and personal way. Because a single person will have the ability to dissuade, disrupt, deny, degrade, and destroy via cyberspace, a hostile individual can seriously harm national security. If the United States is to

ensure security for its citizens, it must create a capable and credible deterrent: cyber omniscience is a viable deterrent.

## Bibliography

- Andrejevic, Mark. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas, 2007.
- Associated Press. "Police Use GM's On Star to Nab Stolen Car." *WWJ-950 News*, 20 October 2009. <http://www.wwj.com/Police-Use-GM-s-OnStar-To-Nab-Stolen-Car/5478318>.
- Batra, N.D. *Digital Freedom: How Much Can You Handle?* New York, NY: Rowman & Littlefield Publishers, Inc., 2008.
- BigDaddySpy.com Free cellular phone GPS software. 17 January 2010.  
<http://store.bigdaddyspy/product-dsblue.htm?gclid=CPG58ZKx1p4CFRafnAodBBkyrA>
- Brate, Adam. *Technomanifestos: Visions From the Information Revolutionaries*. New York, NY: Texere Publishing, 2002.
- Brook, James and Boal, Iain A., eds. *Resisting the Virtual Life: The Culture and Politics of Information*. San Francisco, CA: City Lights, 1995.
- Chilton, Gen Kevin P. "Cyber Leadership: Towards New Culture, Conduct, and Capabilities." *Air and Space Power Journal* 23, no. 3 (Fall 2009): 5-10.
- Clark, Andy. *Natural-Born Cyborgs: Minds, Technologies, and the Future of Human Intelligence*. New York, NY: Oxford University Press, 2003.
- Clark, Wesley K. and Levin, Peter L. "Securing the Information Highway: How to Enhance the United States' Electronic Defenses." *Foreign Affairs* (November/December 2009): 1-7.
- Clarke, Richard A. *Breakpoint*. New York, NY: G. P. Putnam's Sons, 2007.
- Drake, William J., ed. *The New Information Infrastructure: Strategies for U.S. Policy*. New York, NY: The Twentieth Century Fund Press, 1995.
- Friedman, Thomas L. *The World Is Flat: A Brief History of the Twenty-First Century*. New York, NY: Farrar, Straus and Giroux, 2005.
- Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies- and What It Means to Be Human*. New York, NY: Broadway Books, 2004.
- Holy Bible*, New International Version. Grand Rapids, MN: Zondervan Press, 1984.
- Huxley, Aldous. *Brave New World*. New York, NY: Harper & Brothers, 1932.

- Jabbour, Dr. Kamal. "The Science and Technology of Cyber Operations." *High Frontier: The Journal for Space & Missile Professionals* 5, no. 3 (July 2009): 11-15.
- Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military Associated Terms*, 31 October 2009.
- Kramer, Franklin D., Starr, Stuart H., and Wentz, Larry K., eds. *Cyberpower and National Security*. Dulles, VA: NDU Press/Potomac Books, Inc., 2009.
- Kurzweil, Ray. *The Singularity Is Near: When Humans Transcend Biology*. New York, NY: Penguin Books, 2005.
- Library of Congress. "Amazing Grace." Lyrics and history of John Newton's Christian hymn. <http://memory.loc.gov/digli/ihas/html/grace/grace-home.html>.
- Ling, Rich. *The Mobile Connection: The Cell Phone's Impact on Society*. New York, NY: Morgan Kaufmann Publishers, 2004.
- Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York, NY: Basic Books, 1999.
- Lorber, Azriel. *Misguided Weapons: Technological Surprise On the Battlefield*. Washington, DC: Potomac Books, 2002.
- Lord, Kristin M. *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace*. Albany, NY: State University of New York, 2006.
- Lyon, David. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis, MN: University of Minnesota Press, 1994.
- Mitchell, William J. *City of Bits: Space, Place, and the Infobahn*. Cambridge, MA: The MIT Press, 1995.
- . *E-Topia: "Urban Life, Jim – But Not as We Know It."* Cambridge, MA: The MIT Press, 1999.
- Mitrano, Tracy. "A Wider World: Youth, Privacy, and Social Networking Technologies," *EDUCAUSE Review* 4, no. 6 (November/December 2006): 16-19.
- Monahan, Torin, ed. *Surveillance and Society: Technological Politics and Power in Everyday Life*. New York, NY: Routledge Publishers, 2006.
- Montgomery Advertiser*, 19 January 2010.
- Negroponte, Nicholas. *Being Digital*. New York, NY: Alfred A. Knopf, Inc., 1995.

- O'Harrow, Jr., Robert. *No Place to Hide*. New York, NY: Free Press, 2005.
- Okin, J.R. *The Information Revolution: The Not-For-Dummies Guide to the History, Technology, and Use of the World Wide Web*. Winter Harbor, ME: Ironbound Press, 2005.
- Oliver, Richard W. *The Biotech Age*. New York, NY: McGraw Hill, 2003.
- Orwell George. *1984*. New York, NY: Signet Classic, Penguin Group, 1950.
- Paul, T.V., Morgan, Patrick M., and Wirtz, James J., eds. *Complex Deterrence: Strategy in the Global Age*. Chicago, IL: The University of Chicago Press, 2009.
- Rheingold, Howard. *Smart Mobs: The Next Social Revolution (Transforming Cultures and Communities in the Age of Instant Access)*. Cambridge, MA: Perseus Publishing, 2002.
- Scammell, Alison, ed. *I In the Sky: Visions of the Information Age*. London, UK: Aslib/Information Management International, 1999.
- Shachtman, Noah. "26 Years After Gibson, Pentagon Defines 'Cyberspace.'" *Wired*, May 2008. <http://blog.wired.com/defense/2008/05/pentagon-define.html>.
- Shaud, Gen John A. and Lowther, Adam. *Deterring Nonstate Actors*. Research Study. Maxwell AFB, AL: Air Force Research Institute, Air University, 2009.
- Shenk, David. *The End of Patience: Cautionary Notes on the Information Revolution*. Bloomington, IN: Indiana University Press, 1999.
- Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations*. New York, NY: The Penguin Press, 2008.
- Sirak, Michael C. "Game Changers." *Air Force Magazine* (September 2009): 30-38.
- Smart, John. *An Evo Devo Approach to STEEPS (Sci, Tech, Econ, Political, Social) Futures: A Big Picture Foresight Framework for Blue Horizons Leaders*. Lecture presentation to Blue Horizons students, Fall 2009.
- Smith, Stephanie. "Artificial Retina Gives Woman Limited Vision After Decades of Darkness." *CNN.com*, 11 December 2009. <http://www.cnn.com/2009/health/12/11/bionic.eye/index.html>.
- US Department of Defense. *Appropriate Action OSD 111178-09 Academic Year 2009-10 Voluntary Initiative to Leverage Intellectual Capital of DoD Professional Military Education*. Washington, DC: Office of the Secretary of Defense, October 2009.
- Wall Street Journal*, 4 September 2009.

*Webster's New American Dictionary*, New York, NY: Merriam-Webster Publishers, 1995.

Woody Guthrie's official Web site. "This Land Is Your Land." <http://woodyguthrie.org>.

You Tube. "Ella Fitzgerald" and "Memorex."

<http://www.youtube.com/watch?v=Bkt8Dwzl6Sg>.

Zolli, Andrew, ed. *Catalog of Tomorrow: Trends Shaping Your Future*. Indianapolis, IN: Que Publishing, 2003.

## End Notes

1. *The Holy Bible: New International Version* (Grand Rapids, MN: International Bible Society, Zondervan Publishers, 1984), 3.
2. Reference is to the title of Aldous Huxley's *Brave New World*, 1932. This unsettling book foreshadowed a futuristic time of complete totalitarianism. In Cyber Omniscience, a different, yet more comprehensive type of control may be possible.
3. The term deterrence is an expansive one. The author found a widely varied collection of definitions for deterrence in Joint Publications and academic publications, however, settled on "anything that influences an actor not to do something based on the actor's expectation it will get a negative result" as found in *Three Items In One: Deterrence as Concept, Research Program, and Political Issue* by Jeffrey W. Knopf as published in *Complex Deterrence: Strategy in the Global Age* edited by T.V. Paul, Patrick M. Morgan, and James J. Wirtz, (Chicago, IL: The University of Chicago Press, 2009), 31.
4. US Department of Defense, *Appropriate Action OSD 111178-09 Academic Year 2009-10 Voluntary Initiative to Leverage Intellectual Capital of DoD Professional Military Education* (Washington, DC: Office of the Secretary of Defense, October 2009), Tab1, 3.
5. Ibid.
6. Written feedback on Professional Studies Paper from Colonel Christopher J. Kinnan, Deputy Director, Center for Strategy and Technology, 30 November 2009.
7. Ibid.
8. Noah Shachtman, "26 Years after Gibson, Pentagon Defines 'Cyberspace'," *Wired.com*, May 2008), <http://blog.wired.com/defense/2008/05/pentagon-define.html>.
9. Dr. Kamal Jabbour, "The Science and Technology of Cyber Operations," *High Frontier: The Journal of Space and Missile Professionals*, 5, no. 3 (July 2009): 11-15.
10. Seminal thoughts and understanding of deterrence theory largely originate from extensive reading of *Complex Deterrence: Strategy in the Global Age*, edited by T.V. Paul, Patrick M. Morgan, and James J. Wirtz., (Chicago, IL: University of Chicago Press, 2009).
11. *Webster's New American Dictionary*, s.v. "icon" (accessed 3 December 2009).
12. Ibid.
13. Formative thoughts originate in current observations of Bluetooth ear-buds and Richard A. Clarke's *Breakpoint* (London, England: G.P. Putnam's Sons, 2007).
14. *Webster's New American Dictionary*, s.v. "omniscient."
15. Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York, NY: Penguin Books, 2006), 25.
16. This sample list is not intended to be comprehensive and uses cyber terminology common today to provide a frame of reference for the future.
17. Col Kinnan, 30 Nov 09.
18. Free cellular phone GPS software is available from multiple websites including BigDaddySpy.com, <http://store.bigdaddyspy.com/product-p/bdsblue.htm?gclid=CPG58ZKx1p4CFRafnAodBBkyrA>.
19. John Smart, *An Evo Devo Approach to STEEPS (Sci, Tech, Econ, Political, Social) Futures: A Big Picture Foresight Framework for Blue Horizons Leaders*, lecture presentation to Blue Horizons, Fall 2009. Additionally, it is possible for any individual, through such websites as *pipl.com*, to conduct OSINT (Open Source Intelligence) collection.
20. Ibid.
21. Kurzweil, *Singularity*, 7.
22. Ibid., 25.
23. *You Tube*, s.v., "Ella Fitzgerald" and "Memorex", (accessed November 2009) <http://www.youtube.com/watch?v=Bkt8Dwzl6Sg>.
24. Joel Garreau, *Radical Evolution, The Promise and Peril of Enhancing Our Minds, Our Bodies – and What It Means to Be Human*, (New York, NY: Broadway Books, 2005), 1-14.
25. Ibid., 4.

- 
26. Ibid., 15-44.
  27. P.W. Singer. "Robots At War: The New Battlefield." *Wilson Quarterly* (Winter 2009). The lengthy article details many applications of robots on the battlefield. For the purposes of this paper, Singer writes: "Speakers at the United States Army's Annual Strategy Conference at Carlisle Barracks, Pennsylvania in April 2009 reported the United States military has deployed more than 12,000 robots to Iraq and Afghanistan to assist with a variety of combat tasks—search and rescue to explosive ordnance disposal."
  28. Garreau, *Radical*, 53-54, 118 and 120.
  29. Ibid., 122, 130.
  30. Ibid., 6.
  31. Ibid., 12.
  32. Ibid., 130-133.
  33. Ibid., 124-127.
  34. Ibid., 113.
  35. Ibid., 184.
  36. Ibid., 153, credited to Burrhus Frederic "B. F." Skinner.
  37. Andrew Zoll, ed., *Tech TV's Catalog Of Tomorrow* (San Francisco, CA: Que Publishing, 2003), 60-61.
  38. Ibid., 74-88.
  39. Andy Clark, *Natural-Born Cyborgs: Minds, Technologies, and the Future of Human Intelligence* (New York, NY: Oxford University Press, 2003), 59-80.
  40. Paraphrase of *The Holy Bible: New International Version*, Genesis 2:24.
  41. *Catalogue of Tomorrow, Trends Shaping your Future*, 67.
  42. J.R. Orkin, *The Information Revolution: The Not-For-Dummies Guide to the History, Technology, and Use of the World Wide Web* (Winter Harbor, ME: Iron Bound Press, 2005), 35-41. The first four nodes established in 1969 were: University of California Los Angeles (UCLA), Stanford Research Institute, University of California Santa Barbara (UCSB), and the University of Utah.
  43. Ibid., v-ix.
  44. For perspective, the first commercial cellular phones were marketed in the early 1980s and saw limited use. Today, millions are sold every day around the planet as more and more people connect to the global community.
  45. Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-First Century* (New York, NY: Farrar, Straus, and Giroux, 2005), 372-374 and personal experience in Operation Enduring Freedom.
  46. John Newton, "Amazing Grace," Christian hymn first published in 1779. See Bibliography for reference information.
  47. Stephanie Smith, "Artificial Retina Gives Woman Limited Vision After Decades of Darkness," interview with Barbara Campbell, *CNN.com*, 11 December 2009, <http://www.cnn.com/2009/health/12/11/bionic.ey/index.html>.
  48. Written feedback provided by Col Kinnan, 11 January 2010.
  49. Ibid.
  50. Ibid.
  51. Robert O'Harrow, Jr., *No Place to Hide* (New York, NY: Free Press, 2005), 281-287.
  52. *Wikipedia*, s.v. "55th Wing," [http://en.wikipedia.org/wiki/55th\\_Wing](http://en.wikipedia.org/wiki/55th_Wing) (accessed 23 January 2010).
  53. Dr. Jabbour, "Science and Technology," 11-15.
  54. Siobhan Gorman, "How Team Of Geeks Cracked Spy Trade," *Wall Street Journal*, 4 September 2009.
  55. Ibid.
  56. Associated Press, "Police Use GM's On Star to Nab Stolen Car," *WWJ-950 News*, 20 October 2009. <http://www.wwj.com/pages/5478318.php?> (accessed 25 January 2010).
  57. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military Associated Terms*, 157.
  58. Gen John A. Shaud and Adam Lowther, "Deterring Nonstate Actors," (Maxwell AFB, AL: Air Force Research Institute, Air University Press, November 2009), 3.
  59. Ibid., 4-5.
  60. Col Kinnan, 12 January 2010.
  61. George Orwell, *1984* (New York, NY: Signet Classic, Penguin Group, 1950).
  62. Col Kinnan, 12 January 2010.
  63. Unattributed commentary from GeorgeOrwell.com. "1984," <http://georgeorwell.org> (accessed 17 January 2010).
  64. Ibid.
  65. Col Kinnan, 12 January 2010.

- 
66. Jill Nolin, "Traffic Cameras Working Hard in East Montgomery," *Montgomery Advertiser*, 19 January 2010.
67. Ibid.
68. Tracy Mitrano, "A Wider World: Youth, Privacy, and Social Networking Technologies," *EDUCAUSE Review*, 4, no. 6 (November/December 2006): 16-19.
69. Col Kinnan, 12 January 2010.
70. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Dulles, VA: Potomac Books, 2009), 3-23.
71. Col Kinnan, 12 January 2010.
72. Stuart H. Starr, "Toward. A Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer et al. (Dulles, VA: Potomac Books, 2009), 70.
73. Woody Guthrie, "This Land Is Your Land," <http://www.woodieguthrie.org>. Written in 1944, published in 1951. See Bibliography.